

From: [Moody, Dustin \(Fed\)](#)
To: [Kerman, Sara J. \(Fed\)](#)
Subject: Jintai Ding IP Statement -- Re: Selected Algorithms Page
Date: Tuesday, March 29, 2022 3:28:33 PM
Attachments: [image001.png](#)
[image002.png](#)
[image003.png](#)
[DINGJ-CK2D2 \(1\).pdf](#)

He's sending me the hard copy, but also sent me a scan (attached).

I'll work on getting the missing ones.

From: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Sent: Tuesday, March 29, 2022 3:25 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Selected Algorithms Page

Do you have Jintai's? As far as "Selected Algos", we also need

FALCON

Zhenfei Zhang (no IP statement)

SPHINCS+

Bas Westerbaan (no IP statement) joined Round 3

Ward Beullens (no IP statement) joined Round 3

Sara

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Tuesday, March 29, 2022 3:22 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: Re: Selected Algorithms Page

Sounds good.

We'll put the new updated IP statements there too.

Dustin

From: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Sent: Tuesday, March 29, 2022 3:10 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Selected Algorithms Page

So what we have done in the past, is leave Round "x" IP statements on that page as they were for that round. And then, if new people were added, we update the file and put it on the next round page.

However, I think we need IP statements from some people on each algorithm except Dilithium.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Tuesday, March 29, 2022 3:06 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: Re: Selected Algorithms Page

Oh, by the way. We decided to just have the pointer to the team web-pages. The round 3 specs and IP statements can stay where they are on the round 3 page.

Though come to think of it, Jintai will be added as a Kyber member and has an IP statement that is new. Hmm. Maybe we'll include the IP statements as well, but not the submission package.

From: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Sent: Monday, March 28, 2022 2:00 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Selected Algorithms Page

OK, just confirm with the team exactly what we want the menu item title to be.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Monday, March 28, 2022 1:58 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: Re: Selected Algorithms Page

It would be a PDF. Our current text is only about a paragraph long. It's pretty short. I guess it wouldn't have to be a PDF. I think it wouldn't need a call out box - just as long as it's somewhere. Putting it under PQC Standardization (as you did in yellow) looks good to me.

Dustin

From: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Sent: Monday, March 28, 2022 1:55 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Selected Algorithms Page

OK, let me know what the team thinks about the zip and IP files.

To confirm, Jintai will be added to Kyber, correct? Is the joint statement going to be a PDF? Or a page? If the later, maybe we could have it as a subpage under the **PQC Standardization** menu heading. If it's a PDF, we could do a call out box on the Overview and Standardization pages (below)

PQC Standardization

- Call for Proposals
- Example Files
- Round 1 Submissions
- Round 2
- Round 3.....

[Joint IP Statement \(or something\)](#)

Selected Algorithms <- confirmed 3/23

Round 4 Submissions <- confirmed 3/23

Workshops and Timeline

- Etc.
- Etc.

Overview

[Post-Quantum Encryption:
A Q&A With NIST's Matt Scholl](#)

[Post-Quantum Cryptography: the Good, the Bad, and the Powerful](#) (video)

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Monday, March 28, 2022 1:48 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: Re: Selected Algorithms Page

Okay, now I get it. That's a good question. I can see reasons for both ways. I agree that we definitely want the link to their websites. My initial thought would be to leave the zip file and the IP statements as well. I'll ask our team at our meeting tomorrow what they think.

I'm also just thinking of one other thing we might need to post. It's possible we might issue a joint statement regarding IP with Jintai Ding, and maybe CNRS of France. We'd want to have someplace for that too. Any ideas?

From: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Sent: Monday, March 28, 2022 1:43 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Selected Algorithms Page

For reference? Or should they just be left on the Round 3 page as is? Do you just want to have their Website linked in Algorithm Information column.

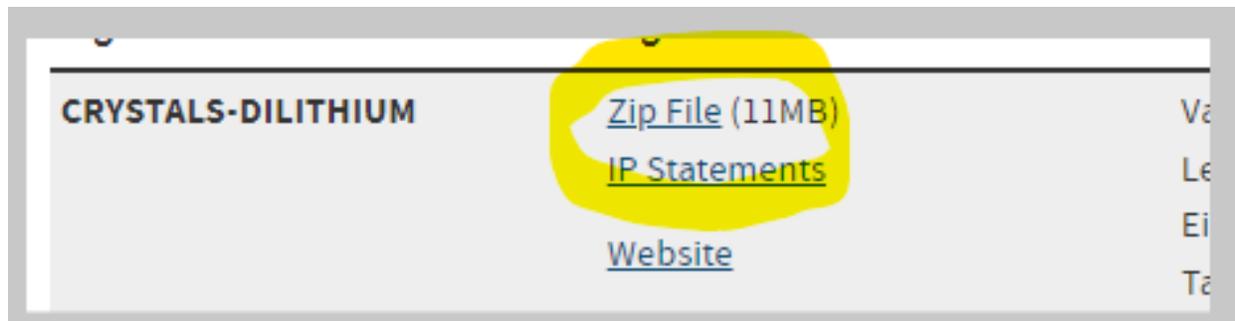
| Algorithm | Algorithm Information |
|--|---|
| Classic McEliece <i>(merger of Classic McEliece and NTS-KEM)</i> | Zip File (97MB) IP Statements Website |

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Monday, March 28, 2022 1:40 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: Re: Selected Algorithms Page

I'm not sure what you mean exactly

From: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Sent: Monday, March 28, 2022 1:39 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Selected Algorithms Page

Hey Dustin,
Should I move the Round 3 zip files and IP statements for the "selected algorithms" page?



| | | |
|---------------------------|---|----------------------|
| CRYSTALS-DILITHIUM | Zip File (11MB) IP Statements Website | Va Le Ei Ta |
|---------------------------|---|----------------------|