From: Moody, Dustin (Fed)
To: Boutin, Chad T. (Fed)
Subject: RE: inquiry / FW: NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals'
Date: Wednesday, January 30, 2019 10:50:00 AM

That answer seems fine. You could add that it will be a small number.

From: Boutin, Chad T. (Fed)
Sent: Wednesday, January 30, 2019 10:48 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: inquiry / FW: NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals'

Hi Dustin,

We got a question via social media: *"Is there a target number of algorithms that they are hoping to winnow down to?"*

Here's my draft answer, please let me know if you want to change anything:

"We don't have a specific target number of algorithms. We do want the group of chosen algorithms to use more than one mathematical approach, as no one is certain what quantum computers' specific capabilities will be."

Thanks,
Chad

From: Esser, Mark (Fed)
Sent: Wednesday, January 30, 2019 10:09 AM
To: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Cc: Stein, Ben (Fed) <benjamin.stein@nist.gov>
Subject: Re: NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals'

Ah, ok, I was looking at the wrong list. Ok, will revise.

"We don't have a specific target number of algorithms. We do want the group of chosen algorithms that use more than one mathematical approach, as no one is certain what quantum computers' specific capabilities will be, so the idea is to cover all bases."

From: Boutin, Chad T. (Fed)
Sent: Wednesday, January 30, 2019 10:04:44 AM
To: Esser, Mark (Fed)
Cc: Stein, Ben (Fed)
Subject: RE: NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals'

Mark,

They don't have a specific target number of algorithms. I do know that in an ideal world they want the group of chosen algorithms to use more than one math approach, as no one is certain what quantum computers' specific capabilities will be, so the idea is to cover all bases.

I'm pretty sure I included math on the GovDelivery lists – might have a glance at the Trello page web posting form. Physics might be stretching it as AFAIK this is purely math-based stuff.

CB

From: Esser, Mark (Fed)
Sent: Wednesday, January 30, 2019 9:53 AM
To: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Cc: Stein, Ben (Fed) <benjamin.stein@nist.gov>
Subject: RE: NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals'

Chad,

We received a comment on FB (https://www.facebook.com/usnistgov/posts/10156998963755365?__xts__[0]=68.ARBtfpJc6temO542nLZnFv_7mPA2bGID2BGPXrAeqZ8bxEf4w8xXzADlDFZpnW4jiEHYP-b_5LJvLh0btuZyOJgt-O0ztCjLnbBlp38we4Xz0z6Uoo-yGg6l35N2jSEx-ZCaamYM3zOb8pROUb3o8JuLYEi-yTTmg7aal0cc8KAt3xY99CM7aFjqrkhEl-kyEwaiJnreILZDrbJjt2n2PJW-9fg9ppxkBK7QNoR3ukOPQCfSotQ4_Chf344zjl27FnV6BmZUbnLcz8KSajYrFSN59CADJEc1VbSQdKyvjwLGmynVzlzHE4DhfP61wmjO1wmnSwuX_dN84fewTaB5&__tn__=-R, hopefully this link works). Is there a target number of algorithms that they are hoping to winnow down to?

Also, for govdelivery, I was going to send to IT and standards, what do you think about adding math and physics?

National Institute of Standards and Technology

www.facebook.com

NIST is narrowing down the candidates for defending against quantum computer attack. Who made the semis? Have a look at the list.