From:	Moody, Dustin (Fed)
To:	Apon, Daniel C. (Fed)
Subject:	FW: illustration draft
Date:	Tuesday, February 12, 2019 1:46:00 PM

From: Boutin, Chad T. (Fed)
Sent: Thursday, December 20, 2018 10:15 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: illustration draft

Dustin – here's an illustration idea that we've put together. Trying to get a few concepts in there: algorithmic math, computer circuitry, selectivity, and the timeframe (which assumes a 12-month investigation round). Any thoughts?

I've asked my editors to get the story draft back to me, and I'll send that to you asap as well.

CB

From: Hanacek, Natasha C. (Fed)
Sent: Thursday, December 20, 2018 10:09 AM
To: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Cc: Stein, Ben (Fed) <benjamin.stein@nist.gov>
Subject: Re: the actual math

Okay, one more version attached with circuit board in the background.

Natasha

From: "Hanacek, Natasha C. (Fed)" <natasha.hanacek@nist.gov>
Date: Wednesday, December 19, 2018 at 2:17 PM
To: "Boutin, Chad T. (Fed)" <charles.boutin@nist.gov>
Subject: Re: the actual math

Is this more along the right lines?

From: "Hanacek, Natasha C. (Fed)" <natasha.hanacek@nist.gov>
Date: Wednesday, December 19, 2018 at 12:10 PM
To: "Boutin, Chad T. (Fed)" <charles.boutin@nist.gov>
Subject: Re: the actual math

Hi Chad,

First draft attached. Let me know if something like this works.

Natasha

From: "Boutin, Chad T. (Fed)" <charles.boutin@nist.gov>
Date: Tuesday, December 18, 2018 at 2:27 PM
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Cc: "Hanacek, Natasha C. (Fed)" <natasha.hanacek@nist.gov>
Subject: RE: the actual math

Yes, that's basically it. FYI I plan to take a few intimidatingly sophisticated-looking math expressions from the part of each supporting doc labeled **Algorithm 1** (etc.) with dark lines above and below (like they used to set off proofs in high-school geometry textbooks, heh) but they will be completely isolated lines. If this is a problem for any reason let me know.

One question:

Could you point out one submission from each of the three families? (I'll draw expressions from each type)

Thanks,
Chad

From: Moody, Dustin (Fed)
Sent: Tuesday, December 18, 2018 1:11 PM
To: Boutin, Chad T. (Fed) <charles.boutin@nist.gov>
Cc: Hanacek, Natasha C. (Fed) <natasha.hanacek@nist.gov>
Subject: Re: the actual math

Chad,

If you go to:

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions

Image removed by sender.

Round 1 Submissions - Post-Quantum Cryptography | CSRC

csrc.nist.gov

Official comments on the First Round Candidate Algorithms should be submitted using the 'Submit Comment' link for the appropriate algorithm. Comments from the

pqc-forum Google group subscribers will also be forwarded to the pqc-forum Google group list...

it is a list of all the submissions. Click on any of them, and you can find the .pdf specification in the Supporting Documents folder. Examples:

Lattices: New Hope, Crystals-Kyber, qTesla, etc....

Code-based: Classic McEliece, BIKE, LEDAkem, etc....

Isogeny-based: SIKE

Multivariate: Rainbow, LUOV, etc...

Hash-based: SPHINCS+, etc....

Is that what you're looking for?

From: Boutin, Chad T. (Fed)
Sent: Tuesday, December 18, 2018 12:31:11 PM
To: Moody, Dustin (Fed)
Cc: Hanacek, Natasha C. (Fed)
Subject: the actual math

Dustin,

We're trying to come up with a decent graphic to accompany the Jan. 10 story we're planning about Post-Quantum Crypto, and we're wondering if you could help us locate some examples of the mathematical formulae that might underlie any or all of the three types of families of algorithms you mentioned to me (lattice, code based and/or multivariant).

In case you're curious, one basic (and purely conceptual) idea will be to put segments of a few formulae into a box representing the submissions, from which the smaller group of candidates will be culled. We just want to make sure anyone in the crypto field who sees the story won't think we're using irrelevant math.

Thanks,
Chad

Chad Boutin
Science Writer
NIST Tech Beat

National Institute of Standards and Technology
301.975.4261

*

“Ah,” said Arthur. “This is obviously some strange usage of the word ‘safe’ that I was previously unaware of.”