From:	Chen, Lily (Fed)
To:	Moody, Dustin (Fed)
Subject:	Re: Comments on PQC Article
Date:	Monday, February 11, 2019 3:14:37 PM

Hi, Dustin,

Thanks.

Lily

From: Dustin Moody <dustin.moody@nist.gov>
Date: Monday, February 11, 2019 at 3:12 PM
To: Lily Chen <lily.chen@nist.gov>
Subject: RE: Comments on PQC Article

Lily,
I've talked with Ray, and made the changes he suggests. See the attached version. He said he's signed off on it.

Dustin

From: Perlner, Ray (Fed)
Sent: Monday, February 11, 2019 2:54 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Comments on PQC Article

Ok. It looks like you didn't take up all my suggested changes (e.g. you're still referring to the SHA1 attack which was not publicly implemented until 2016 as a "practical attack" in 2005, and you didn't update the text on security definitions as much as I would have liked), but you did get the most important ones.

On, rereading, I also noticed that this sentence on page 3

"For example, an improper padding method can leak information about the private key."

is probably supposed to be a reference to the Bleichenbacher attack – but that recovers an RSA plaintext, not an RSA private key. There are reaction attacks on postquantum schemes that recover the private key, but they typically have more to do with failure to prove knowledge of the plaintext, or failure to check error distributions than padding schemes as such.

In any event, I think I can sign off on the document as it stands, but you might want to consider further changes.

Ray

From: Chen, Lily (Fed)
Sent: Monday, February 11, 2019 7:41 AM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: FW: Comments on PQC Article

Hi, Ray,

You can check this version. Thanks,

Lily

From: Dustin Moody <dustin.moody@nist.gov>
Date: Monday, February 11, 2019 at 7:35 AM
To: Lily Chen <lily.chen@nist.gov>
Subject: Re: Comments on PQC Article

Lily,

I made the corrections that Ray suggested. Please find the attached updated versions.

Dustin

From: Chen, Lily (Fed)
Sent: Thursday, February 7, 2019 5:01:08 PM
To: Perlner, Ray (Fed); Moody, Dustin (Fed)
Subject: RE: Comments on PQC Article

Hi, Ray,

Thanks. We will work on the comments.

Lily

From: Perlner, Ray (Fed)
Sent: Thursday, February 07, 2019 4:28 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Comments on PQC Article

Page 1: “The hardness of the integer factorization and discrete logarithm problems is believed to provide sufficient

security for applications utilizing classical computing technology."

This is incorrect. It implies that RSA and DH are secure as long as they run on a classical computer. What's important is what kind of computer the adversary has. Suggest changing to

"The hardness of the integer factorization and discrete logarithm problems is believed to provide sufficient security, as long as they can only be attacked using classical computing technology."

Page 2: "One example is the McEliece cryptosystem [9]. It is based on the hardness of decoding a general linear code, which is classically known to be hard and seems immune to Shor's quantum attack."

There are a few questionable claims in this sentence. First of all McEliece is not proven secure based on the assumption that decoding a general linear code is hard. Existing security proofs also make the assumption that a disguised Goppa code is computationally indistinguishable from a general linear code. This is not known to be true, and in some extreme cases it is known to be false. Second of all, no problem on which cryptography is based is "known to be classically hard" as P=?NP remains unresolved.

Page 2: "The internal state must be carefully managed to ensure that each private key can be used only once to generate a signature."

This sentence doesn't have enough context. The previous sentences need to make clear that the internal state of the signer's machine must manage a series of one-time private keys, and that if any one of them is reused, the resulting signatures give enough information for an attacker to forge signatures.

Page 3: "Among these various categories, some are relatively new while others are based on ideas known for many years."

It is unclear from context what "these various categories" refers to.

Page 3: "Performance is not only counted by an algorithm's processing speed but also the memory requirement: key sizes, data expansion rate (i.e. ciphertext size), signature size etc."

Key sizes (with the exception of the private key) really have more to do with communication overhead than memory requirements (On pretty much any platform a megabyte of communication is a big deal for crypto, a megabyte of memory may not be.) Memory requirements are really properly a separate consideration from public key, ciphertext, and signature sizes.

Page 4: "In 2005, the first practical attack on SHA-1 was presented."

Generally, "practical attack" means someone actually implemented it. The attack was not implemented (that we know of) prior to 2016. Perhaps change to "better-than-brute-force attack".

Page 4: "functinality"
Should be "functionality". Note I'm not proofreading that carefully, so don't take this as exhaustive.

Page 5:" The NIST call for proposals encourages security proofs against well accepted security definitions. It requires semantically secure encryption or key encapsulation with respect to adaptive chosen ciphertext attack (IND-CCA2) and existentially unforgeable digital signatures with respect to an adaptive chosen message attack (EUF-CMA)."

Strictly speaking there isn't anything untrue about the above. But, the primary point of the security definitions was to define what constitutes an attack, rather than to ask for security proofs (which we encourage, but do not require.)

Page 5: "The notion of secure against chosen plaintext attack (CPA) can be used for encryption or key establishment if it is to be employed in a purely ephemeral-key protocol."
We probably shouldn't shorten "IND_CPA" since we didn't shorten the others.
"The call for proposals also allows for the consideration of encryption and key establishment schemes that are only

semantically secure against chosen plaintext attack (IND_CPA) if they are to be employed in a purely ephemeral-key protocol."

Page 6: "The NIST call for proposals states the desire of optimized methods in addressing side-channel attacks, including choosing algorithms with constant-time implementation."
This sentence is very awkwardly worded and possibly incorrect or misleading. Try
"The NIST call for proposals encourages the incorporation of countermeasures such as constant-time implementation in optimized code, so that measured performance will more meaningfully reflect the performance of a secure implementation."

Page 7: "As a result, some design team submitted two versions of their algorithm."

Should be "some design teams"

Page 7: The selection of the second-round candidates was based on taking into account of the security, cost and performance, and implementation characteristics of each submitted algorithm.

Middle part should be "…taking into account the security…" (the word "of" should be removed after "account").